SECURE ROAMING BETWEEN WIRELESS ACCESS POINTS

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit, under 35 U.S.C. § 365 of International Application PCT/US04/02491, filed January 29, 2004, which was published in accordance with PCT Article 21(2) on November 4, 2004 in English and which claims the benefit of United States provisional patent application No. 60/458,189, filed March 27, 2003.

TECHNICAL FIELD

[0001] This invention relates to wireless local area networks, and particularly to methods and systems that facilitate roaming between wireless access points on a wireless access network.

[0002]

BACKGROUND OF THE INVENTION

[0003] IEEE 802.11-based wireless local area networks (WLANs) have become the focus of much research and development in recent years. WLANs offer simple, convenient to use, high throughput ways in which portable computer users can break away from the tethers of the wired world and move around freely with comparable network throughput. However, when a user moves from one access point to another, there is a need to provide seamless roaming. Present technology does not adequately meet this requirement.

[0004] In most of the current deployment, IEEE 802.11 uses static Wired Equivalent Privacy (WEP) keys and does not support per user session keys, thus, the wireless stations, usually clients, and all access points participating in roaming can have the same static WEP key. However, the security problem with static WEP keys has been highly publicized. Further, static WEP key protocols do not solve the distribution of authorization information to a large number of access points. To solve this problem, the IEEE 802.11 standard is trying to develop an Inter Access Point Protocol (IAPP).

[0005] The IEEE 802.1x standard addresses the security problem in IEEE 802.11 by using port controlled access control. In a large 802.1x installation, a backend authentication server authenticates the user. In order to secure the wireless link, the wireless station must go through an authentication process involving the station, the access point and the authentication server. If authentication is successful, a session key is agreed upon between the wireless station and the access point. This solution enables roaming, but with high overhead, i.e., each

time a station is associated with a different access point, for example because of signal fluctuation, the whole authentication process has to be carried through. This is highly undesirable, especially when the authentication server is far away from the wireless LAN, e.g., in an inter-working environment where the WLAN is in, for example, JFK airport but the authentication server belongs to, for example, SBC in California.

[0006] There is a need to provide seamless roaming when a wireless user (client) wishes to switch to an access point with better signal strength.

[0007] There is also a need to move per-user session keys and authorization information from one access point to another when a client roams between wireless access points.

[0008]

SUMMARY OF THE INVENTION

[0009] These needs and others, which will become apparent from the following disclosure are met by the present invention which comprises in one aspect a wireless local area network comprising gateway to control multiple access points. The access points reside in a wired or other type of network. The gateway is programmed to receive session data requests from access points, look up session data, and send session data back to the requesting access points. The access points are programmed to send requests for session data to the gateway and to receive and process session information setting commands from the gateway. The system comprising such a gateway moves the "intelligence" of the wireless network into such gateway and results in very simple access points, which enables easier control and more economical installation for large deployments.

[00010] In another aspect, the invention comprises a method of, and computer readable medium for, enabling roaming of wireless clients among wireless access points in a network comprising providing a gateway in the network, sending session data requests from access points to the gateway, looking up session data stored in the gateway, reporting session data failure if session data is not found, and sending a session data response from the gateway to the access points if session data is found or is generated by the gateway.

[00011] The present invention can compliment the IEEE 802.1x protocol and greatly reduce the complexity of the protocol.

[00012] The basic architecture of the system of the invention is illustrated in Fig. 1 wherein a gateway is used to control a number of access points with simple functions. The access points can be directly connected to the gateway or can be connected to the gateway

through a network. Besides the normal IEEE 802.11 physical layer and MAC layer functions, these access points need only to support the following additional functions:

[00013] Per station session key;

[00014] An interface to accept session information (e.g. session key and authorization information) setting commands from the gateway; and

[00015] The capability to query the gateway about session information and transfer session information from the gateway.

[00016] Among these things, the first function is already widely available on many access points on the market presently. The other two functions are novel.

[00017] The invention also provides methods to deal with session information on the access point the wireless station (client) previously associated with, after the client roams to a different access point. In a first method, the gateway informs the previous access point to remove the information. In a second method, the access point sets up a timer to remove all idle wireless station entries after a certain time period of inactivity. The second method is preferred because the gateway does not have to send an extra command to remove the entry and the AP may maintain the entry to deal with "thrashing" scenarios in which the wireless station oscillates between two or more access points rather quickly. Because the entry is already there, the access point may just inquire the gateway about the "freshness" of the information instead of transferring all the session information. This may not seem to be significant if the session information only contains the session key, but with large session information, this could be potentially faster and save bandwidth.

[00018] There are differences in handling, or transferring, session information generated at the access point versus session information generated at the gateway.

[00019] The session information must be transferred to the gateway, thus the gateway must provide an interface for accepting session information, and the access point must be enhanced with the capability of transferring session information to the gateway. This is illustrated in Figure 3.

[00020] When session information is generated at the gateway, the session information need be transferred to the access point that the wireless station is associated with. There are no additional functionalities required at the access point beyond the basic functions mentioned earlier.

[00021] For the scheme to be secure, it must be ensured at any time that the connection between the gateway and each AP is trusted. This can be ensured through either physical security or encryption.

[00022] Physical security requires directly attaching the access points to the gateway or through a managed network.

[00023] Encryption requires that upon initial installation and configuration, the gateway and access points share a secret, or the gateway shares a secret with each access point. The communication between the gateway and the access points are encrypted with the secret(s).

[00024] For large deployment of this invention and to facilitate faster roaming, multiple gateways can be organized in a hierarchy. Each gateway is responsible for a number of access points. When the wireless station roams among the access points belonging to the same gateway, session transfer is controlled by this gateway. Only when the station associates with the WLAN the first time or when it roams across access points belonging to different gateways, would it be necessary for the gateway to fetch session information from the gateway in the higher hierarchy.

[00025]

BRIEF DESCRIPTION OF DRAWINGS

[00026] Fig. 1 illustrates an embodiment of a system of the invention having a gateway in the wired network, the wired network comprising access points.

[00027] Fig. 2 illustrates a flow chart of a first example of an authentication and association process among a wireless station, an access point, and a gateway according to the invention.

[00028] Fig. 3 illustrates a second example of an authentication and association process among a wireless station, an access point, and a gateway according to the invention.

[00029] Fig. 4 illustrates a third example of an authentication and association process among a wireless station, an access point, and a gateway according to the invention.

[00030]

DETAILED DESCRIPTION

[00031] Referring first to Fig. 1, an embodiment of a system according to the invention is illustrated wherein access points 11, 12, and 13 are connected to a wired network 14. There is no limit to the number of access points in the wired network. A smart gateway 15 is connected to the wired network 14. Wireless clients, such as laptop computers 16 and 17 and

personal data assistants 18 and 19 are illustrated as communicating with the access points 11, 12, 13. Present generation clients and access points use 802.11 protocols.

[00032] Referring next to Fig. 2, a process is illustrated wherein a wireless station 16 requests an association with an access point 11 during step 20. The access point 11 which relays the session data request to the gateway 15 during step 21. During step 22, the gateway 15 looks up the session data and if session data is not found during step 23, a session data failure signal is relayed during step 24 to the access point 11, which then generates session data during step 25 and sends the generated session data during step 26 to the gateway 15 and also sends an association response to the wireless station 16 during step 27.

[00033] The session information (including session key and authorization information) can be generated at the access points, as illustrated in Fig. 2, or at the gateway, as illustrated in Fig. 3, wherein the wireless station 16 requests an association with an access point 11 during step 20. The access point relays the session data request to the gateway 15 during step 21. The gateway 15 looks up the session data during step 22 and if session data is not found during step 23, the gateway generates the session data during step 28, and sends a session data response back to the access point 11 during step 29. The access point 11 loads the session data during step 30, and sends the association response back to the wireless station 16 during step 27.

[00034] As illustrated in the Fig. 2, Fig. 3, and Fig. 4, the access point first checks with the gateway to see if session information already exists for the wireless station. If session information does not already exist, as illustrated in Figs. 2 and 3, the wireless station is not authenticated by the WLAN yet or the previous authentication has expired. The normal authentication steps are carried out and session information (including the session key) is generated for the station and is set in both the currently associated access point and the gateway.

[00035] If session information already exists, for example, when the wireless station roams from one access point to another, the gateway returns it to the access point. The access point sets that information (including the session key) in the access point. An example of such a process is illustrated in Fig. 4 wherein the wireless station 16 sends the association request to access point 11 during step 20, which relays the session data request to the gateway 15, which in turn looks up the session data during step 22 and finds it. The access point sends a session data during step 29 to the access point 11 which then loads the session data during step 30 and sends an association response to the wireless station 16 during step 27.

[00036] This simple procedure ensures that session information travels with the wireless station from one access point to another without the station having to go through authentication all over again.

[00037] Thus the invention described herein provides a secure wireless local area network infrastructure for seamless roaming with smart gateways and simple access points.

[00038] While the invention has been described in detail herein, various alternatives, modifications, and improvements should become readily apparent to those skilled in theis art without departing from the spirit and scope of the invention.